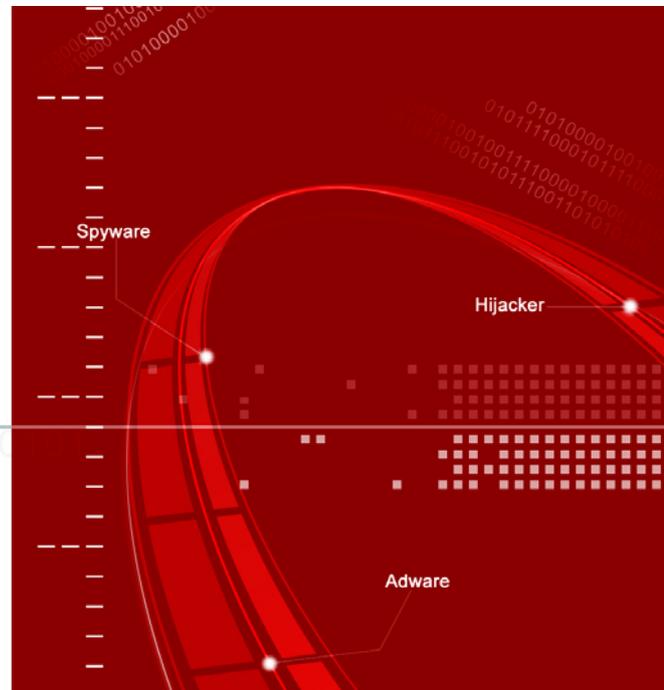


EVERYZONE

TurboVaccine *AI*

바이러스 진단 · 치료 전문백신

사용설명서



EveryZone

Copyright© (주)EveryZone 1994-2006 All Rights Reserved.

목 차

1장. 터보백신 Ai의 소개	4
1. 터보백신에 대하여	4
2. 주요 특징	5
2장. 터보백신 Ai의 구성	9
1. 메인 화면	9
2. 메뉴 바	10
3. 툴 바	13
4. 검사 영역	14
5. 현재 설정 상태 영역	15
3장. 터보백신 Ai의 사용 방법	18
1. 바이러스 검사 방법	18
2. 바이러스 치료 방법	19
3. 백신 업데이트 방법	21
4. 백업파일 복원기 사용 방법	22
5. 예약설정 사용 방법	25
6. E-mail 감시기 사용 방법	27
7. 환경 설정 방법	28

터보백신 Ai의 소개

터보백신에 대하여 / 4

주요 특징 / 5

터보백신 설치의 배경과
주요 특징을 소개합니다.

터보백신에 대하여

1994년 4월에 나온 DOS용(TV.EXE) 터보백신은 1994년 10월 국내 최초의 **Windows**용 백신으로 변모하며, 네티즌 여러분의 많은 사랑을 받아 왔습니다. 이 터보백신이 21세기를 맞이하여 새롭게 변모했습니다. 예전의 이미지 그대로 강력한 기능을 보유하고 손쉬운 사용법으로 사용자 편의성을 극대화했습니다.

주요 특징

터보 바이러스 추적 엔진(Turbo Virus Tracing Engine) 탑재

독자적으로 개발한 가상 실행 엔진을 이용하여 바이러스를 실행해 가면서 추적하는 방식으로 신뢰도 높고 정확한 진단율과 치료율을 보여 줍니다.

운영체제 차원의 실시간 감시기능

사용자가 직접 실시간 감시 수준을 설정하여 실시간으로 내부 또는 외부로부터 유입되는 바이러스를 100% 차단하며, 최적화된 설계로 매우 적은 수준의 리소스 점유합니다.

인터넷 감시기능

인터넷 상으로 유입되는 파일들을 실시간으로 감시하여 차단할 수 있습니다.

실시간 전자우편 첨부파일 감시기능

독자적으로 개발한 POP3 Proxy 를 통하여 Outlook, Netscape, Eudora 등의 메일 클라이언트로부터 유입되는 바이러스를 실시간으로 차단하며 매우 적은 수준의 리소스를 점유합니다.

신뢰도 높은 치료 기술

윈도우 시스템이 현재 사용 중인 파일도 치료 가능하며, 어떠한 감염된 파일이라도 도스용 안티-바이러스 프로그램 사용없이 100% 치료 가능한 윈도우 환경에 최적화된 진단/치료 합니다.

다양한 압축 파일 검사 기능 제공

ACE, ARJ, BZ2, CAB, GZ, LHA, RAR, TAR, ZIP, ZOO로 압축된 압축 파일 검사기능을 지원하며 무한대의 다중 압축파일 검사 기능을 제공합니다.

빠르고 손쉬운 인공지능 원격 업데이트 기능

최초 설치 후 자동으로 원격 업데이트가 이루어지므로 사용자는 업데이트에 신경을 쓸 필요가 없습니다.

직관적이고 편리한 사용자 인터페이스

사용자가 가장 많이 사용하는 기능들을 편리하게 배치하고, 단순화시키는 사용자 친화적인 GUI를 사용하여 컴퓨터 비전문가라도 쉽게 사용가능합니다.

EVERYZONE

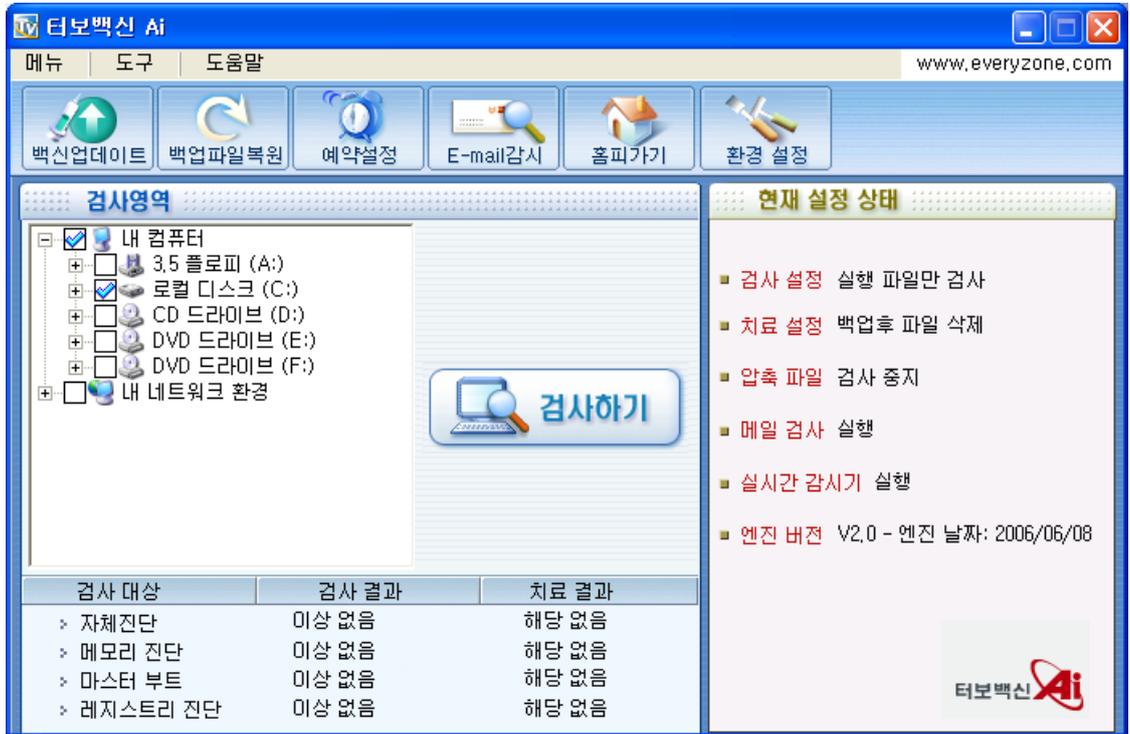
터보백신 Ai의 구성

메인 화면 / 9
메뉴 바 / 10
툴 바 / 13
검사 영역 / 14
현재 설정 상태 영역 / 15

터보백신 화면 구성을
영역별로 소개합니다.

메인 화면

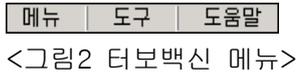
터보백신 Ai는 기본적으로 메뉴바, 툴바, 검사 영역, 현재 설정상태 영역으로 나누어 집니다.



<그림1 터보백신 메인화면>

메뉴 바

메뉴도구, 도움말 등으로 구성되어 있으며 대부분의 기능을 이곳에서 선택하여 사용할 수 있습니다.



메뉴의 구성



<그림3 트레이 메뉴>

터보백신 실행

터보백신 Ai 메인창이 나타납니다.

시스템 감시 중지

현재 동작하고 있는 실시간 감시 기능을 일시 중지합니다.

예약 설정 실행

지정한 시간과 날짜에 바이러스 검사와 최신 엔진 업데이트를 받을 수 있도록 설정하는 기능을 담당합니다.

e-mail 감시 설정

아웃룩과 같은 개인 메일 프로그램을 설치하여 사용하는 경우 메일로 유입되는 바이러스를 미리 차단해 줍니다.

터보백신 업데이트

수동으로 최신 터보백신으로 업데이트 할 수 있습니다.

종료

터보백신 Ai를 종료합니다.

도구의 구성



<그림4 도구에뉴>

환경 설정

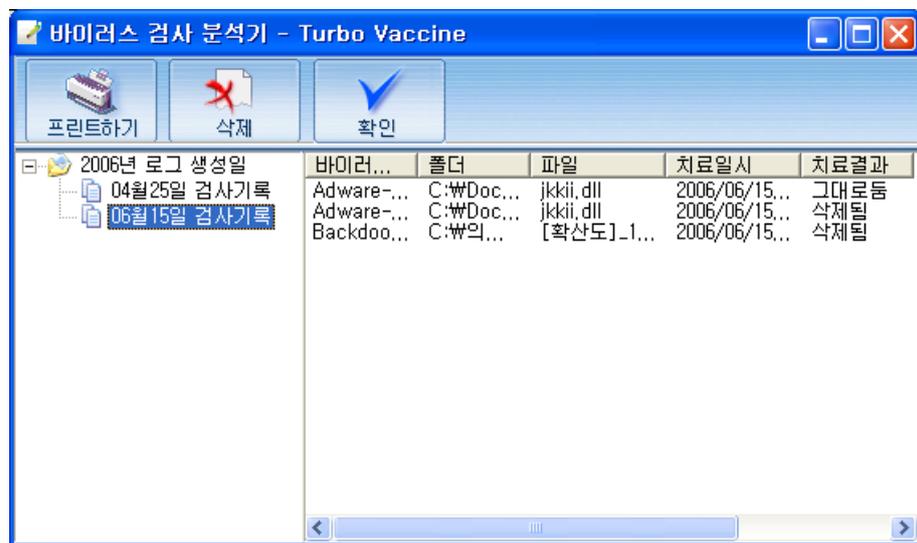
바이러스 검사 시 적용되는 옵션을 지정할 수 있습니다.

복구 디스크 만들기

바이러스 등의 피해로 부트영역 정보가 손상되어 부팅이 안 될 경우를 대비해서 복구 디스크를 만듭니다.

바이러스 검사 분석

바이러스 검사기록 로그를 확인할 수 있습니다.



<그림5 바이러스 검사 분석기>

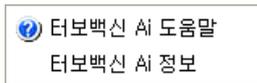
바이러스 정보

발견된 바이러스에 대한 정보를 웹을 통해 확인 할 수 있습니다.

바이러스 활동일지

바이러스가 활동하는 날짜를 웹을 통해 확인하여 불의의 피해를 예방 할 수 있습니다.

도움말의 구성



<그림6 도움말 메뉴>

터보백신 Ai 도움말

터보백신의 사용방법을 알려줍니다.

터보백신 Ai 정보

사용자와 제품 버전을 확인할 수 있습니다.

터보백신에서 가장 사용빈도가 높은 기능을 위주로 배치하여 해당 버튼을 클릭하는 것으로 터보백신의 주요 기능을 간편하게 사용할 수 있습니다.



<그림7 툴바>

백신 업데이트

이 버튼을 클릭하시면 항상 최신 터보백신으로 업데이트할 수 있습니다.

백업 파일 복원

바이러스 치료 시에 감염된 파일을 암호화하여 보관하게 됩니다. 단 이 기능은 환경설정->치료설정 부분에서 [치료시 이전 파일을 보관합니다] 옵션을 체크해주셔야 합니다.

예약 설정

지정한 시간과 날짜에 바이러스 검사와 최신 엔진 업데이트를 받을 수 있도록 설정 하는 기능을 담당합니다.

E-mail 감시

아웃룩과 같은 개인 메일 프로그램을 설치하여 사용하는 경우 메일로 유입되는 바이러스를 미리 차단해줍니다.

환경 설정

바이러스 검사 시 적용되는 옵션을 지정할 수 있습니다.

검사 영역

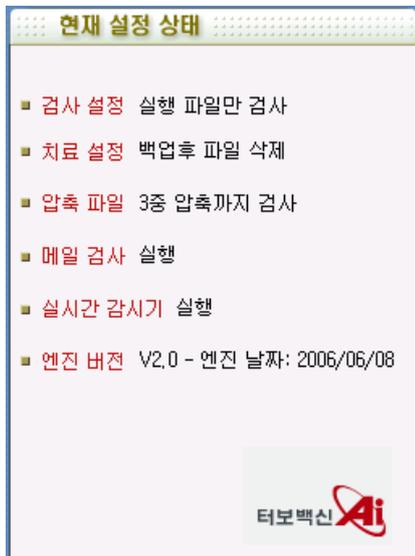
트리 부분에 사용자님의 하드 디스크가 표시되며 검사 버튼과 자체 진단, 메모리 진단, 마스터 부트, 레지스트리 진단 결과를 리포트 형식으로 보여 줍니다.



<그림8 검사 영역>

현재 설정 상태 영역

바이러스 검사 시 적용되는 모든 옵션을 표시 해주며 현재 설치되어 있는 터보백신의 엔진 버전을 확인하여 항상 업데이트 여부를 확인할 수 있습니다.



<그림9 현재 설정 상태>

EVERYZONE

터보백신 Ai의 사용방법

바이러스 검사 방법 / 18

바이러스 치료 방법 / 19

백신 업데이트 방법 / 21

백업 파일 복원기 사용 방법 / 22

예약 설정 사용 방법 / 25

E-mail 감시기 사용 방법 / 27

환경 설정 방법 / 28

터보백신의 사용 방법을

기능별로 소개합니다.

바이러스 검사 방법

트리 영역에서 원하는 하드 디스크나 폴더를 선택합니다.



<그림10 트리 영역>

상태는 **로컬 디스크(C:)**를 선택한 모습입니다. 기호를 클릭하면 폴더를 선택할 수 있습니다.

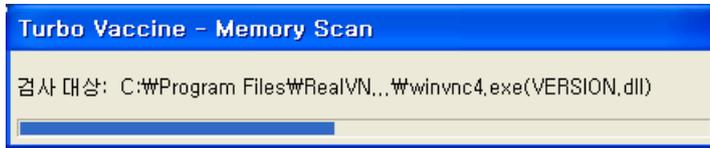


<그림11 검사하기 버튼>

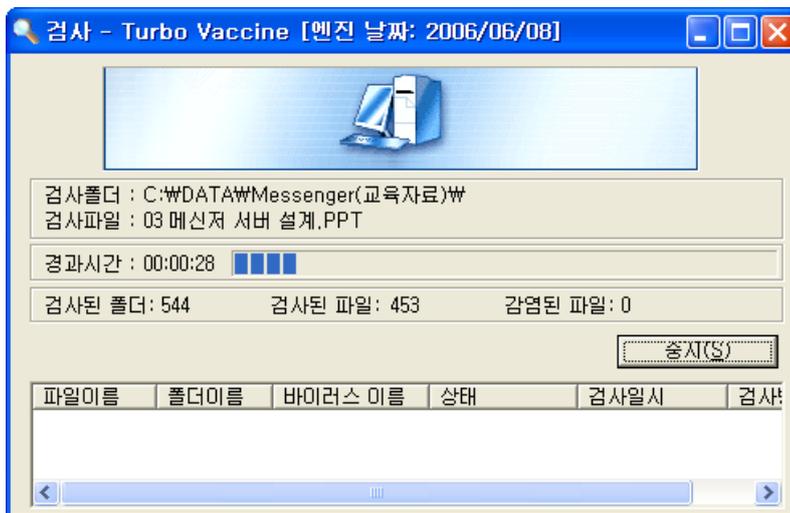
이 상태에서 검사하기 버튼을 클릭하시면 로컬 디스크(C:) 바이러스 검사를 시작합니다. 바이러스 검사는 환경 설정 옵션의 영향을 받습니다. 현재 환경설정 상태 영역에서 확인하신 후 환경 설정 메뉴에서 옵션을 변경할 수 있습니다.

바이러스 치료 방법

1. 검사를 시작 하면 다음과 같은 창이 뜨게 됩니다.

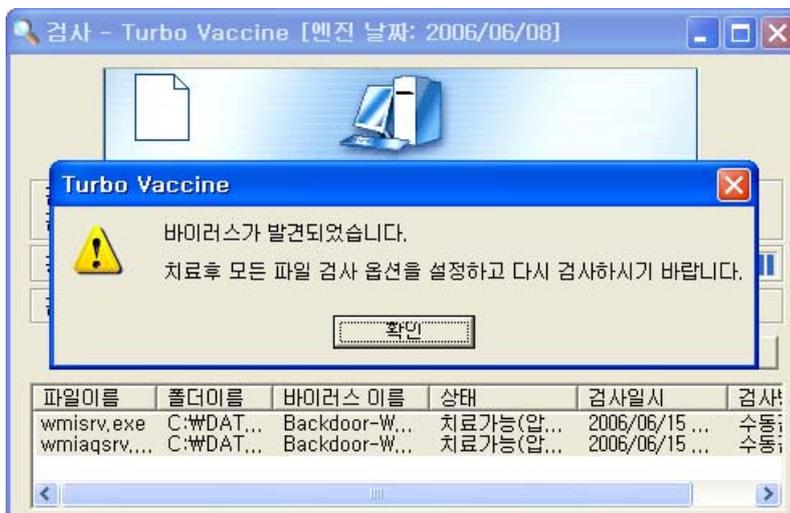


<그림12 메모리 검사>



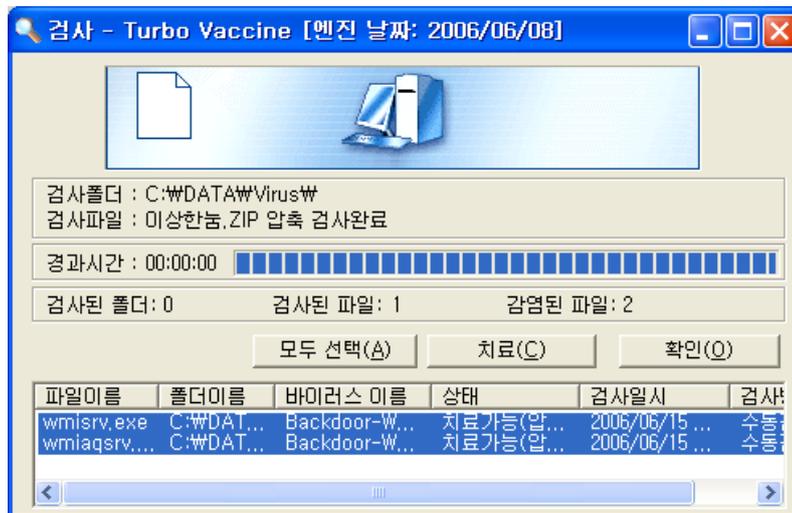
<그림13 바이러스 검사>

2. 이 상태에서 바이러스를 발견하면 다음과 같은 창이 뜨게 됩니다.



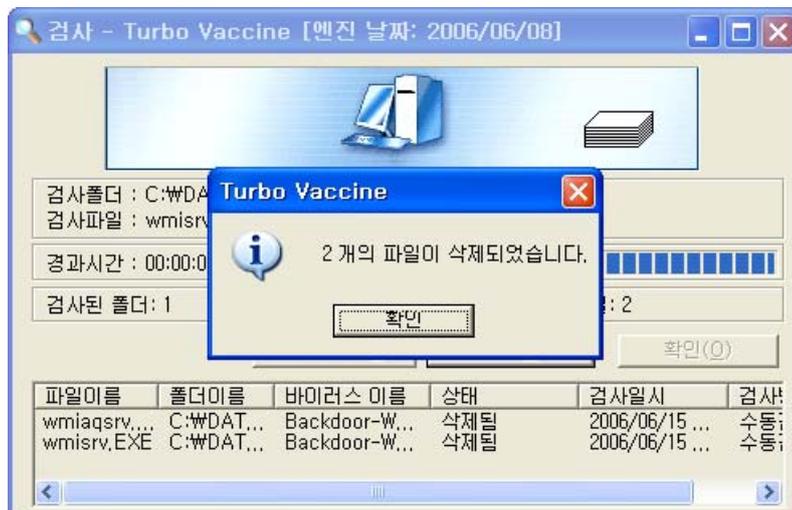
<그림14 바이러스 발견>

3. 바이러스를 발견하면 모두 선택 버튼을 클릭합니다. 또는 CTRL 키나 SHIFT 키를 이용하여 치료할 파일을 개별적으로 선택 할 수 있습니다.



<그림15 바이러스 치료1>

4. 치료 버튼을 클릭하면 바이러스 치료가 완료됩니다.



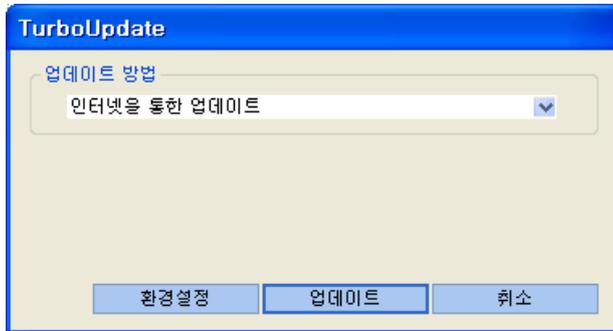
<그림16 바이러스 치료2>

주의사항

바이러스 치료 후에는 치료된 파일이 환경설정 옵션에 따라 자동 저장됩니다. 이 파일은 백업파일 복원 메뉴를 사용 하시면 다시 복원할 수 있습니다.

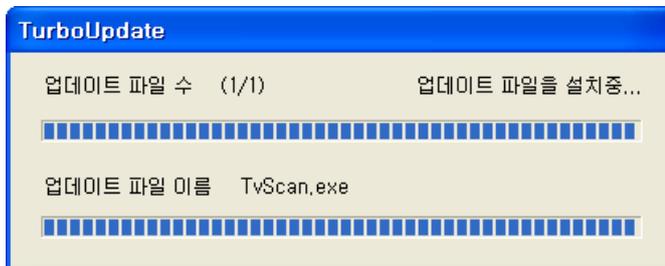
백신 업데이트 방법

1.  버튼을 클릭하면 다음과 같은 업데이트 박스가 나옵니다.



<그림 17 업데이트1>

2. [업데이트] 버튼을 클릭하면 **EveryZone** 업데이트 서버에서 가장 빠른 서버를 자동으로 확인하여 신속하게 최신 바이러스 엔진을 업데이트 합니다.

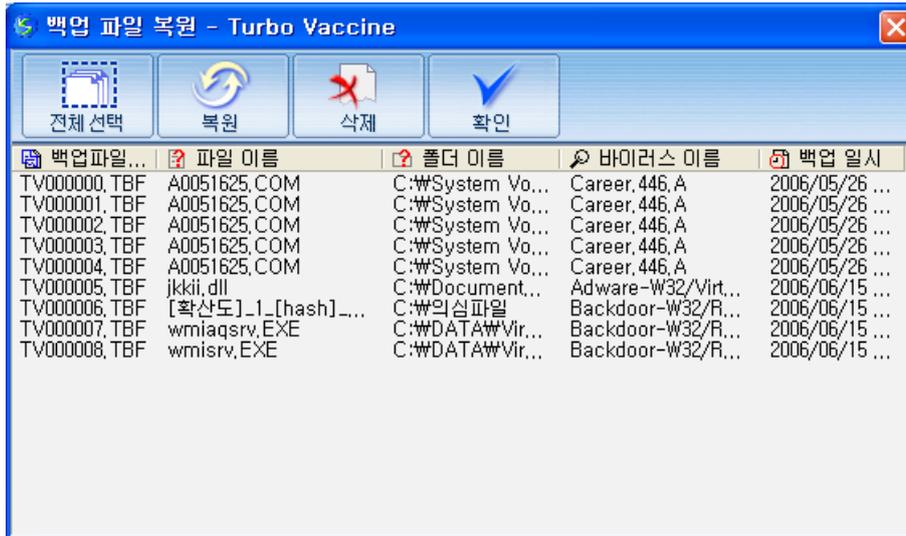


<그림 18 업데이트2>

백업 파일 복원기 사용 방법



버튼을 클릭하면 다음과 같은 백업파일 복원기 박스가 나옵니다. 이 때 한번이라도 터보백신으로 바이러스를 치료한 상태라면 백업파일 복원기는 다음과 같이 실행될 것입니다.

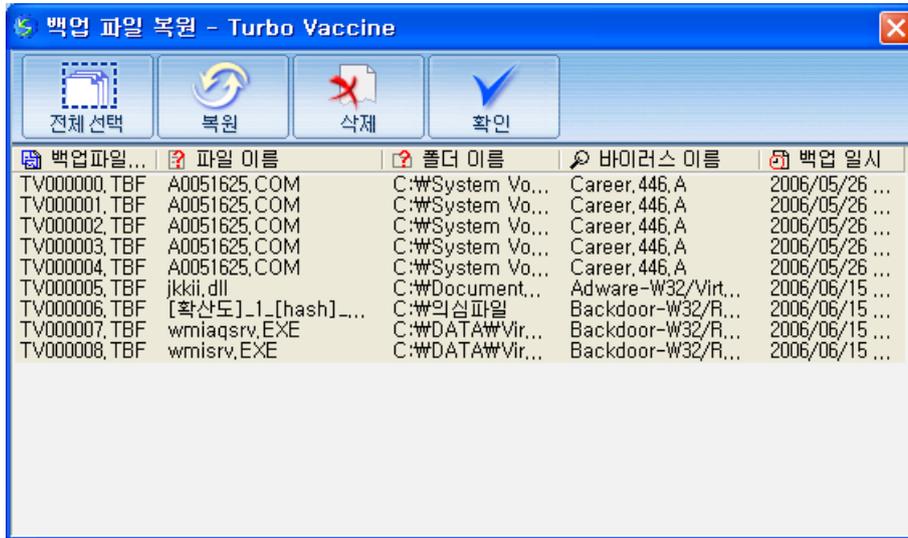


<그림19 백업 파일 복원1>

위 그림에서 Tv000000.TBF는 감염된 파일을 터보백신 고유파일 포맷으로 만들어서 저장한 형태로 바이러스의 동작을 하지 못합니다. 이 파일들은 터보백신 Ai 가 설치된 폴더의 **_Restore**폴더에 존재하게 됩니다. 만일 중요한 문서나 파일을 복구할 필요성이 있을 때는 다음과 같은 절차에 따라 진행하시면 파일을 복원할 수 있습니다. 먼저 복구하기를 원하는 파일을 개별적으로 선택(CTRL키나 SHIFT키 이용) 하거나 또는 전체 선택 버튼을 이용합니다.

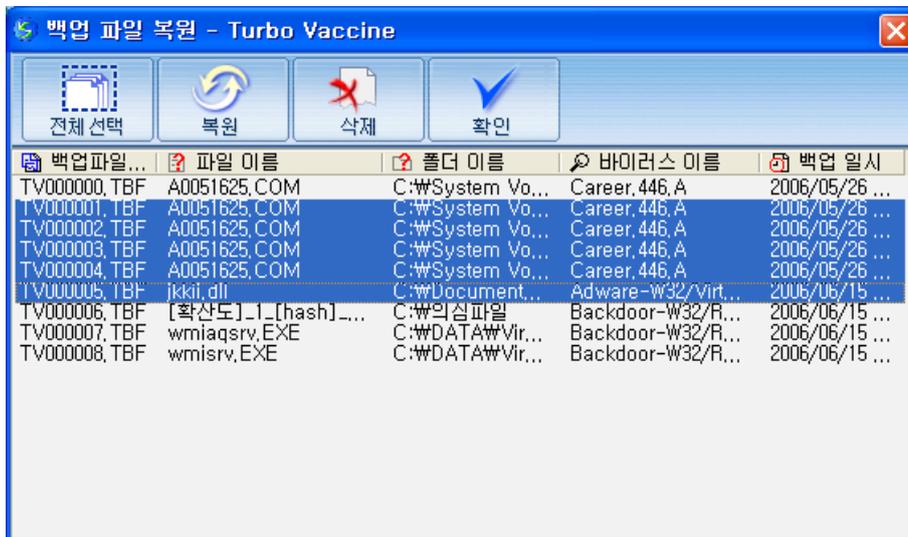


버튼을 이용했다면 다음과 같이 박스가 표시될 것입니다.



<그림20 백업 파일 복원2>

만약 개별적으로 선택되었을 때에는 다음과 같이 박스가 표시될 것입니다.



<그림21 백업 파일 복원3>

이러한 상태에서  버튼을 클릭하면 선택한 파일을 원래의 상태로 복원하게 됩니다. 아래 상태는 전체 선택을 했을 때 나타나는 박스이며 개별적으로 파일을 선택했을 때에도 동일하게 나타납니다.



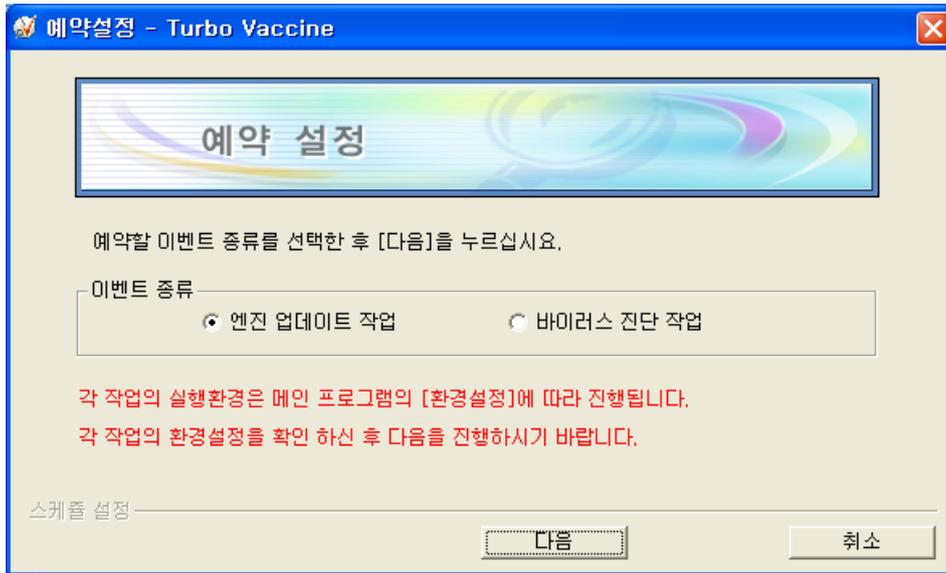
<그림22 백업 파일 복원4>

주의사항

백업파일 복원기로 파일을 복원하더라도 치료 이전의 상태로 복원되므로 바이러스에 감염되어 있는 상태입니다. 그러므로 파일을 복원할 경우에는 신중을 기하셔야 합니다.

예약 설정 사용 방법

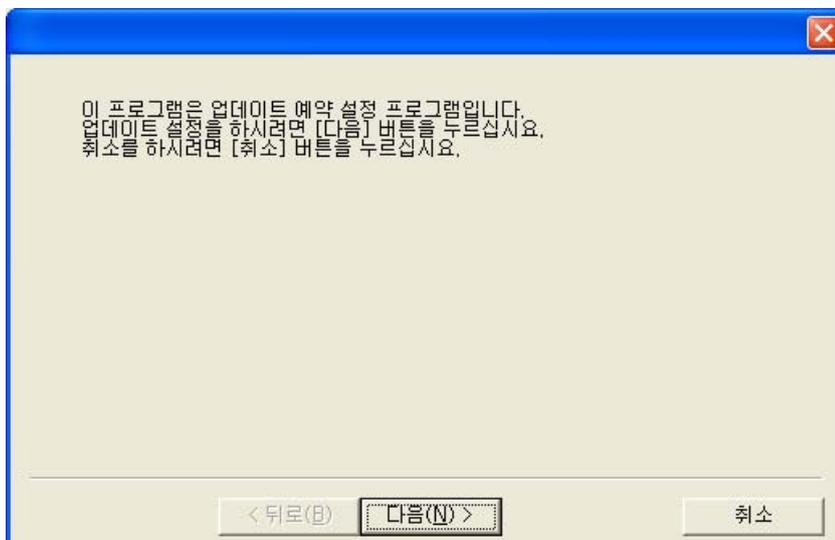
1. 툴바 메뉴에서  버튼을 클릭하면 다음과 같은 박스가 나타납니다.



<그림23 예약 설정1>

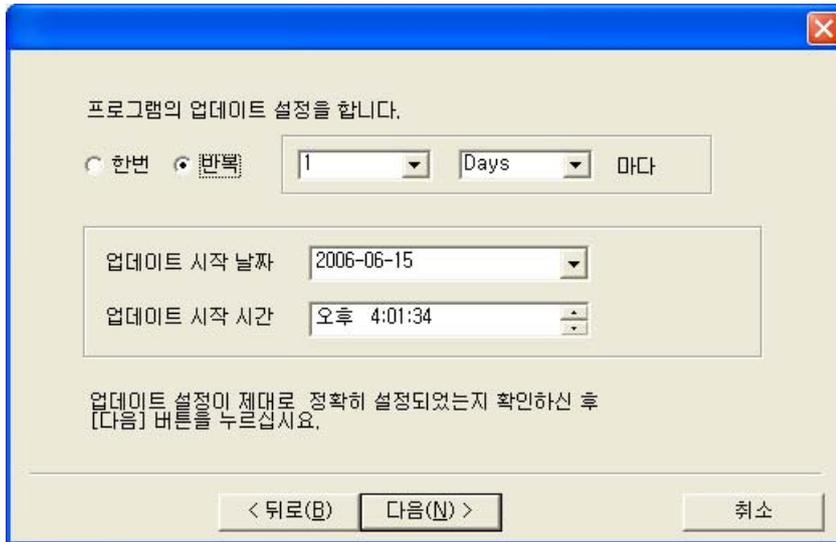
이벤트 종류 중에 "바이러스 진단 작업"과 "엔진 업데이트 작업" 항목이 있는데 원하는 항목을 선택합니다.

2. 만약 엔진 업데이트 작업을 선택했고 [다음] 버튼을 클릭했다면 다음과 같은 박스가 나타날 것입니다.



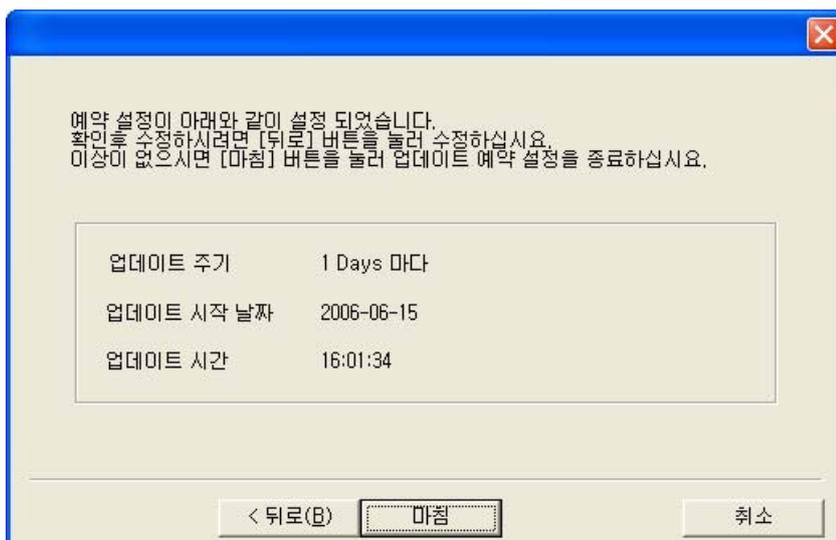
<그림24 예약 설정2>

3. 다음 박스에서는 해당 이벤트를 한번만 실행 할 것인지 아니면 주기적으로 실행 할 것인지를 결정합니다. “**한번**”만 선택한다면 이벤트를 지정한 시간에 한번 수행 하지만 “**반복**”을 선택하면 지정한 시간부터 분, 시간, 요일 단위 등으로 주기적인 수행을 하게 됩니다. “**업데이트 시작 날짜**” 항목은 오전, 오후, 시간, 분, 초 단위로 세밀하게 조정할 수 있습니다. “**업데이트 시작 시간**” 또한 년, 월, 일 단위로 세밀하게 조정 가능합니다.



<그림25 예약 설정3>

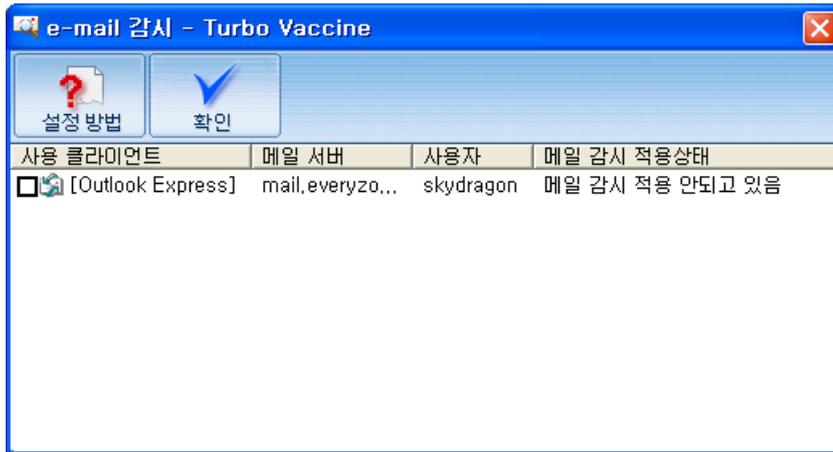
4. 다음은 이벤트 설정 결과입니다.



<그림26 예약 설정4>

E-mail 감시기 사용 방법

1. 툴바 메뉴에서  버튼을 클릭하면 다음과 같은 박스가 나타납니다. 만약 메일 프로그램을 사용하고 있는 경우라면 다음과 같은 화면이 나타날 것입니다. 이 화면은 사용자님의 계정에 따라 다르게 표시 됩니다.

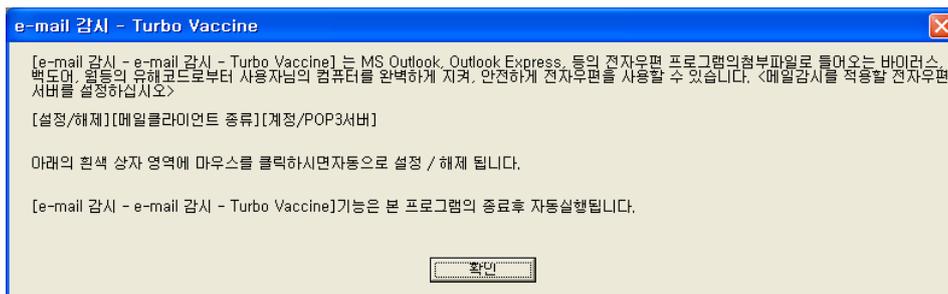


<그림27 E-mail 감시기1>

이 상태는 현재 사용하고 있는 메일 프로그램이 Outlook Express 이며 에브리존 계정을 사용하고 있다는 것을 표시해 줍니다. 이 상태에서 부분을 클릭하면 메일로 유입되는 바이러스를 차단할 준비가 된 것입니다.

2. 그런 다음  버튼을 클릭하시면 비로소 이메일 감시기가 동작하게 되며 아웃룩 실행 시 메일로 유입되는 바이러스를 실시간으로 차단하게 됩니다.

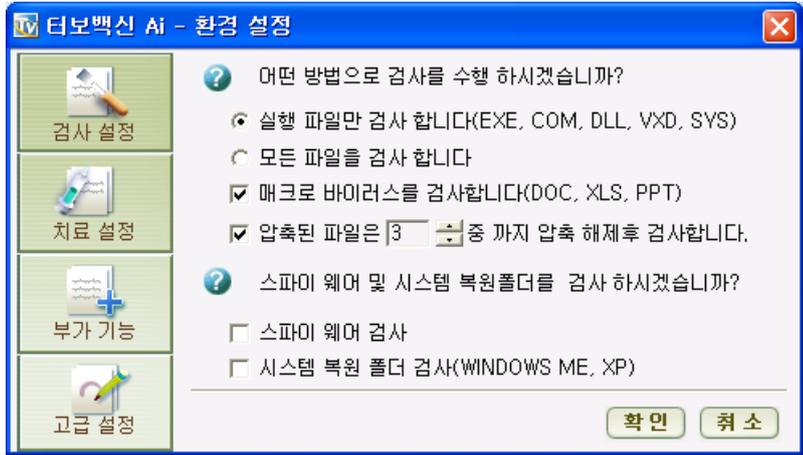
3.  버튼을 클릭하면 e-mail 감시기에 대한 간단한 도움말이 나옵니다.



<그림28 E-mail 감시기2>

환경 설정 방법

툴바 메뉴에서  버튼을 클릭하면 다음과 같은 박스가 나타납니다.



<그림27 환경설정-검사설정>

버튼

검사 설정, 치료 설정, 부가 기능 설정, 고급 설정 등 모든 옵션을 지정하고 나서 이 버튼을 클릭해야만 바뀐 옵션이 바이러스 검사할 때 적용됩니다.

버튼

환경설정 옵션을 변경했다 하더라도 취소 버튼을 클릭하면 기존의 환경 설정 정보는 그대로 유지 됩니다.



버튼

이 설정에서는 검사할 파일의 종류와 스파이웨어를 검사할지를 선택 합니다. 이 설정은 모든 바이러스 검사 시에 적용됩니다.

실행 파일만 검사 합니다.(EXE, COM, DLL, VXD, SYS)

이 옵션을 선택 하면 가장 빠른 바이러스 검사를 수행할 수 있는 장점이 있는 반면에 실행 파일만을 검사하므로 일반적인 파일에 감염된 바이러스는 진단을 하지 못하는 단점이 있습니다.

모든 파일을 검사 합니다.

이 옵션을 선택하면 하드 디스크에 존재하는 모든 파일을 하나하나 검사하여 바이러스를 정확히 잡아내는 장점이 있는 반면에 바이러스 검사 시간이 실행 파일만 검사하는 경우에 반하여 오래 걸리는 단점이 있습니다.

매크로 바이러스를 검사 합니다.(DOC, XLS, PPT)

이 옵션은 실행 파일만을 검사할 때 따로 선택을 하여 실행 파일검사와 매크로 바이러스 검사를 동시에 진행 시킬 수 있습니다. 그러나 모든 파일 검사 옵션을 선택했을 경우에는 따로 옵션을 지정하지 않아도 매크로 바이러스를 동시에 검사합니다.

압축 파일 검사

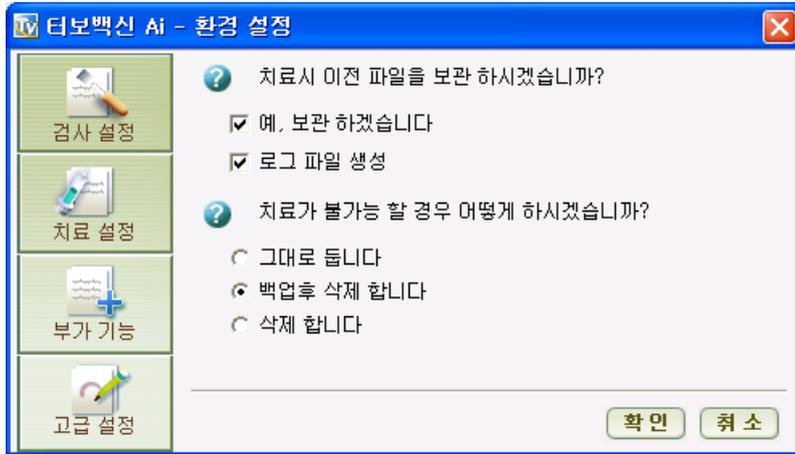
이 옵션은ACE, ARJ, BZ2, CAB, GZ, LHA, RAR, TAR, ZIP, ZOO로 압축된 압축 파일 검사기능을 지원하며 무한대의 다중 압축 파일 검사 기능을 제공합니다.

스파이웨어 검사

이 옵션을 클릭하면 사용자 정보를 유출하는 프로그램을 검출할 수 있습니다. 자세한 정보는 에브리존 홈페이지 [바이러스 FAQ] 27번 문서를 참고하시기 바랍니다.



버튼



<그림28 환경설정-치료설정>

이 설정에서는 검사된 바이러스의 치료 방법을 설정해 줍니다. 이 설정은 모든 바이러스 치료 시에 적용됩니다.

예, 보관 하겠습니다.

이 옵션을 클릭하면 발견된 바이러스를 치료할 경우에 파일이 자동으로 보관됩니다. 보관된 파일은 “백업파일 복원”기를 사용하여 언제든지 원래의 상태로 복원할 수 있습니다. 이 옵션은 [백업파일 복원기능 사용방법] 을 참고하시기 바랍니다.

그대로 둡니다.

치료가 불가능할 경우, 감염된 파일을 삭제하지 않고 그대로 둡니다.

백업 후 삭제 합니다.

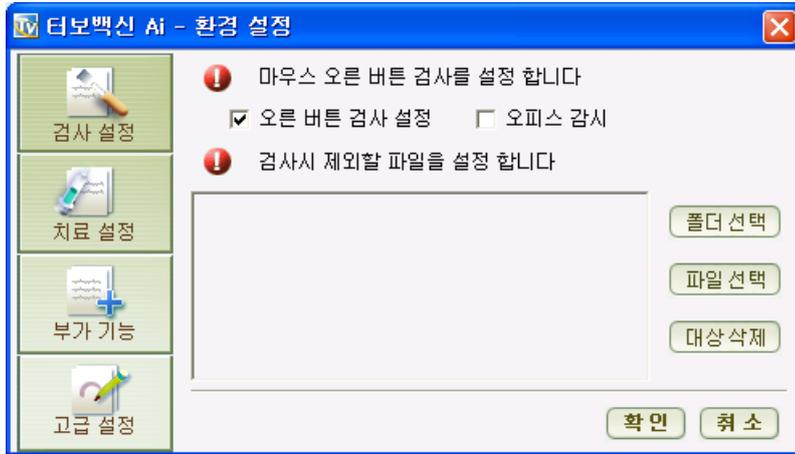
치료가 불가능할 경우에는 감염된 파일을 백업 후 삭제 합니다. 이 때 백업한 파일은 “백업파일 복원”기를 이용하여 다시 원래의 상태로 복원할 수 있습니다.

삭제 합니다.

치료가 불가능할 경우에는 감염된 파일을 영구적으로 하드디스크에서 삭제합니다. 이렇게 삭제된 파일은 다시 복구할 수 없습니다.



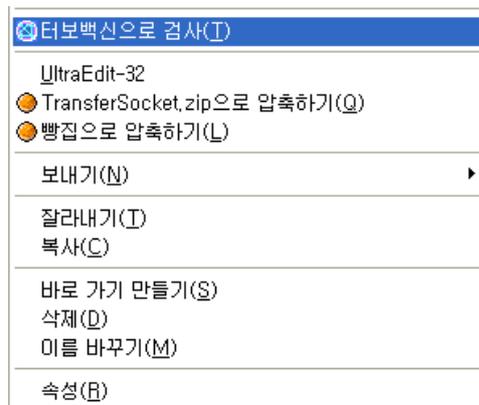
버튼



<그림29 환경설정-부가기능>

오른 버튼 검사 설정

마우스 오른 버튼 검사 설정을 통해서 터보백신 Ai를 실행 시켜 바이러스 검사를 하지 않아도 간편하게 바이러스 검사를 할 수 있습니다. 오른 버튼을 파일이나 폴더에 클릭하면 다음과 같이 나타납니다.



<그림30 팝업메뉴>

탐색기나 바탕 화면에서 검사하고자 하는 파일이나 폴더를 선택하여 마우스 오른 버튼을 클릭한 다음 “터보백신으로 검사(T)”를 클릭하면 바이러스 검사를 시작합니다.

검사 시 제외할 파일을 설정

바이러스 검사시에 제외할 파일이나 폴더를 등록해두면 바이러스 검사를 더욱 빨리 끝낼 수 있습니다. 단, 여기에 포함될 파일이나 폴더는 사용자가 바이러스로부터 안전하다고 판단되는 것이어야 합니다.

파일 선택 버튼

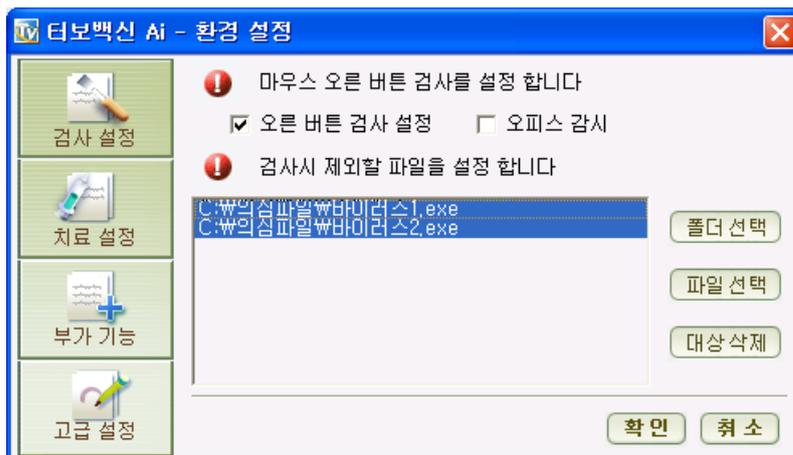


<그림33 파일열기>

파일을 선택하여 [열기(O)] 버튼을 클릭하면 다음과 같이 파일이 추가됩니다. SHIFT키나 CTRL키를 누른 상태에서 마우스를 클릭하면 여러 개의 파일을 한꺼번에 선택할 수 있습니다.

대상 삭제 버튼

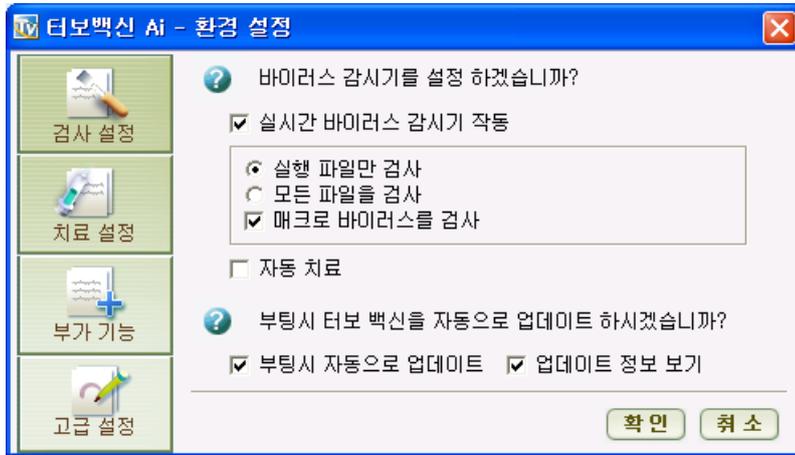
이 버튼을 클릭하면 제외할 목록의 리스트를 삭제할 수 있습니다. SHIFT키나 CTRL키를 누른 상태에서 마우스를 클릭하면 여러 개의 목록을 한꺼번에 선택할 수 있습니다.



이 후로는 바이러스 검사 시에 해당 파일과 폴더를 검사하게 됩니다.



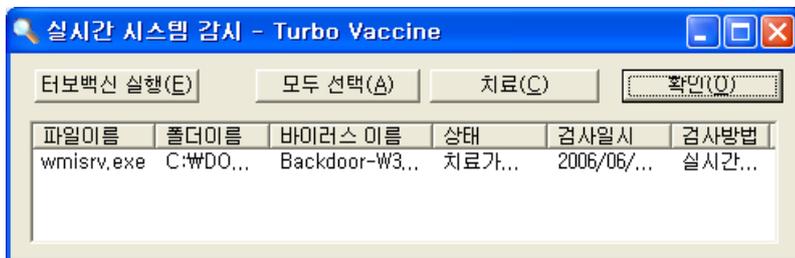
버튼



<그림34 환경설정-고급설정>

실시간 바이러스 감시기 작동

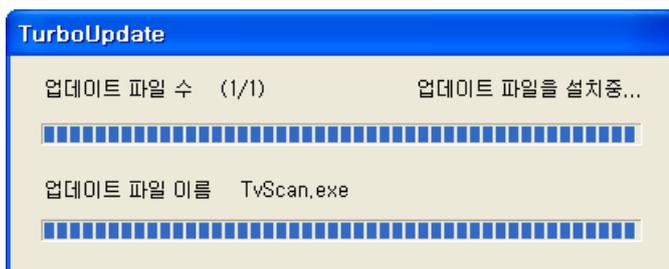
사용자가 직접 실시간 감시기를 설정하여 실시간으로 내부 또는 외부로부터 유입되는 바이러스를 100% 차단하며, 최적화된 설계로 매우 적은 수준의 리소스를 점유하여 시스템에 무리를 주지 않고 바이러스를 검사할 수 있습니다.



<그림35 실시간 감시>

부팅 시 자동으로 업데이트

부팅할 때마다 새로운 터보백신 Ai 바이러스 진단 치료 엔진을 EveryZone 업데이트 서버에서 확인 하여 업데이트 받을 수 있습니다.



<그림36 업데이트>

EVERYZONE